

IN THE ABSTRACT

Add the Abstract appearing on the following separate sheet:

ABSTRACT

A method for the secure application of a cryptographic algorithm of the RSA type in an electronic component obtains the value of a public exponent e from a given set of probable values, without a priori knowledge of that value. Having determined the value for the public exponent e , the application of countermeasures using the value of e , to block error attacks and side channel attacks, particularly of the DPA and SPA type, are carried out on the application of a private operation of the cryptographic algorithm.